

Alan Charles LLOYD, *et al.*
Serial No. 10/705,242
December 15, 2008

AMENDMENTS TO THE CLAIMS:

The following listing of claims supersedes all prior versions and listings of claims in this application:

1-138. (Cancelled)

139. (New) A method for storage and retrieval of directory data in a directory system running on at least one processor having access to at least one data storage device and at least one communications network with interfaces to at least one application running on other processors having need of directory system services, said method comprising:

running plural intelligent directory service modules as a part of said directory system, said intelligent directory service modules comprising at least one of (a) an identity management module, (b) a presence management module, and (c) a messaging management module;

storing data objects used by the directory service modules in respectively corresponding different organized logical segments of memory, each segment containing

Alan Charles LLOYD, *et al.*
Serial No. 10/705,242
December 15, 2008

object attribute data needed by the corresponding directory service module to perform its intelligent service in response to an incoming request;

receiving directory service requests from said application(s) running on said other processors, said requests including an identification of the type of requested directory service comprising at least one of (a) identity service, (b) presence service, and (c) messaging service;

directing received directory service requests to the directory service module respectively corresponding to the identified type of requested directory service; and

returning responses to incoming requests based on the outputs of at least one intelligent directory service module without requiring access of other object attribute data separately stored for another of the intelligent directory service modules.

140. (New) A method as in claim 139, wherein said directory system comprises at least three intelligent directory service modules including at least: (a) an identity management module, (b) a presence management module, and (c) a messaging management module.

Alan Charles LLOYD, *et al.*
Serial No. 10/705,242
December 15, 2008

141. (New) A method as in claim 139, wherein said intelligent directory service modules provide customized virtual machines within said directory service.

142. (New) A method as in claim 139, wherein data storage and processing methods practiced by said intelligent directory service modules are embodied within solid state integrated circuits.

143. (New) A method as in claim 139, wherein said different organized logical segments of memory containing object attribute data associated with corresponding different intelligent directory services are, in turn, logical segments of memory providing a directory information tree (DIT).

144. (New) A method as in claim 143, wherein said DIT is used to locate the logical segment of memory corresponding to the requested intelligent directory service and to access the object attribute data associated therewith.

Alan Charles LLOYD, *et al.*
Serial No. 10/705,242
December 15, 2008

145. (New) A method as in claim 139, wherein said object attribute data includes data indicating whether each of said attributes is associated with one or more other attributes.

146. (New) A method as in claim 139, wherein said attribute data includes data indicating whether each of said attributes is a sponsoring attribute for one or more other attributes.

147. (New) A method as claimed in claim 139, wherein attributes having directory object naming characteristics in common are stored together.

148. (New) A method as in claim 147, wherein the directory object naming characteristics correspond to one of: distinguished name attributes, aliased distinguished names, and non-naming attributes.

149. (New) A method as in claim 139, wherein one of the intelligent directory services provides security services and uses its own security attribute data corresponding

Alan Charles LLOYD, *et al.*
Serial No. 10/705,242
December 15, 2008

to one of: collective attributes, compound attributes, attributes of compound attributes, X.500/LDAP operational attributes, user operational attributes, sponsoring attributes.

150. (New) A method as in claim 139, wherein said segments include a first segment for storing distinct name binding rules, access control information, object schema and management data for said directory objects.

151. (New) A method as in claim 150, wherein one of the intelligent directory services provides configuration services with said schema and management data to configure said object attribute data according to processing requirements of said intelligent directory services.

152. (New) A method as in claim 143, wherein:
the directory system generates a directory operation access control identifier for use in determining whether a user is granted access to perform a selected directory operation on a selected attribute type in a selected portion of a DIT, said directory operation access control identifier identifying said directory operation, said portion of said DIT and said attribute type, and

Alan Charles LLOYD, *et al.*
Serial No. 10/705,242
December 15, 2008

the directory system determines whether said access is granted on the basis of a comparison of said directory operation access control identifier with one or more access control identifiers associated with one or more of said portion of said DIT, said attribute type, and an attribute type group including said attribute type.

153. (New) A method as in claim 139, wherein:

the directory system is adapted to generate one or more access control identifiers for a user on the basis of access configuration information for a user, and

a trusted operating system is used to determine said user's access to a directory object on the basis of access control identifiers associated with said object and said user.

154. (New) A method as in claim 139, wherein said memory segments includes transaction segments dedicated to storage of transaction data representing phases of a directory transaction to allow recovery of said directory transaction.

155. (New) A method as in claim 139, including an adaptation component for automatically reconfiguring said memory segments on the basis of usage of said memory segments.

Alan Charles LLOYD, *et al.*
Serial No. 10/705,242
December 15, 2008

156. (New) A method as in claim 139, wherein said memory segments include at least one adaptation segment dedicated to storage of adaptation data representing the usage of said memory segments.

157. (New) A method as in claim 156, wherein said adaptation data represents the organization of directory data stored in said memory segments.

158. (New) A method in claim 155, wherein said reconfiguring includes segregating one or more portions of said directory data on the basis of access frequencies for said one or more portions of said directory data.

159. (New) A method as in claim 155, wherein said reconfiguring includes segregating one or more portions of directory data based on the number of instances of an entity of said directory data in a region of memory.

Alan Charles LLOYD, *et al.*
Serial No. 10/705,242
December 15, 2008

160. (New) A method as in claim 155, wherein said reconfiguring includes segregating instances of an attribute type from a name space into two or more regions of memory.

161. (New) A method as in claim 139, including modules for accessing and managing said plurality of memory segments.

162. (New) A method as in claim 161, including a composite attribute module for managing composite attributes and extracting from said composite attributes particular attributes for storage in an associated object attribute data segment.

163. (New) A method as in claim 161, including a statistical module for generating statistical data in relation to directory entries.

164. (New) A method as in claim 161, including a monitoring module for monitoring one or more directory entries and for generating notification data in response to modification of a monitored directory entry.

Alan Charles LLOYD, *et al.*
Serial No. 10/705,242
December 15, 2008

165. (New) A method as in claim 161, including a collective attributes module for segregating collective attributes of entries within a name space.

166. (New) A method as in claim 161, including a X.509 certificate validation module for validating one or more certificate paths.

167. (New) A method as in claim 161, including a multi-object management module for processing two or more objects as an entity.

168. (New) A method as in claim 167, wherein said two or more objects include a sponsoring object and one or more sponsored objects.

169. (New) A method as in claim 168, wherein said multi-object management module is adapted to automatically generate said one or more sponsored objects when a sponsoring object is generated.

Alan Charles LLOYD, *et al.*
Serial No. 10/705,242
December 15, 2008

170. (New) A method as in claim 169, wherein said multi-object module is adapted to automatically generate one or more objects related to a user object when said user object is generated.

171. (New) A method as in claim 170, wherein said user object represents a user, and said one or more objects represent one or more services for said user.

172. (New) A method as in claim 139, including a service authorization module for determining whether a user is authorized to use one or more services.

173. (New) A method as in claim 172, wherein said service authorization module is adapted to perform said determining in response to a directory search.

174. (New) A method as in claim 173, wherein said directory search is based on an authorization matching rule, service and device properties, and an authorization token.

Alan Charles LLOYD, *et al.*
Serial No. 10/705,242
December 15, 2008

175. (New) A method as in claim 139, including a relational search module for performing a distributed object relational search in response to a search query including relational operators.

176. (New) A method as in claim 139, wherein the identity-based service components include a user presence management component that maintains presence attributes of said users, said presence attributes including an attribute that indicates whether a user is using a directory.

177. (New) A method as in claim 176, wherein said user presence management component generates one or more events in response to a change in said user presence attributes for each user.

178. (New) A method as in claim 139, wherein the message-based service component includes a message transfer component that enables the message attributes of said directory objects to be transferred to other directory objects.

Alan Charles LLOYD, *et al.*
Serial No. 10/705,242
December 15, 2008

179. (New) A method as in claim 139, including at least one attribute processor adapted to store and process attribute data of a directory.

180. (New) A method as in claim 179, wherein said attribute processor includes an application-specific integrated circuit.

181. (New) Computer-readable storage media storing executable computer program code which, when executed, performs the method of claim 139.

182. (New) Apparatus for storage and retrieval of directory data comprising a directory system running on at least one processor having access to at least one data storage device and at least one communications network with interfaces to one or more applications running on other processors having need of directory system services, said apparatus comprising:

plural intelligent directory service modules running as a part of said directory system, said intelligent directory service modules comprising at least one of (a) an identity management module, (b) a presence management module, and (c) a messaging management module;

Alan Charles LLOYD, *et al.*
Serial No. 10/705,242
December 15, 2008

memory storing data objects used by the directory service modules in respectively corresponding different organized logical segments of memory, each segment containing object attribute data needed by the corresponding directory service module to perform its intelligent service in response to an incoming request;

at least one data input receiving directory service requests from said application(s) running on said other processors, said requests including an identification of the type of requested directory service comprising at least one of (a) identity service, (b) presence service, and (c) messaging service;

means for directing received directory service requests to the directory service module respectively corresponding to the identified type of requested directory service;
and

means for returning responses to incoming requests based on the outputs of at least one intelligent directory service module without requiring access of other object attribute data separately stored for another of the intelligent directory service modules.

183. (New) Apparatus as in claim 182, wherein said directory system comprises at least three intelligent directory service modules including at least: (a) an identity

Alan Charles LLOYD, *et al.*
Serial No. 10/705,242
December 15, 2008

management module, (b) a presence management module, and (c) a messaging management module.

184. (New) Apparatus as in claim 182, wherein said intelligent directory service modules provide customized virtual machines within said directory service.

185. (New) Apparatus as in claim 182, wherein data storage and processing methods practiced by said intelligent directory service modules are embodied within solid state integrated circuits.

186. (New) Apparatus as in claim 182, wherein said different organized logical segments of memory containing object attribute data associated with corresponding different intelligent directory services are, in turn, logical segments of memory providing a directory information tree (DIT).

187. (New) Apparatus as in claim 186, wherein said DIT is used to locate the logical segment of memory corresponding to the requested intelligent directory service and to access the object attribute data associated therewith.

Alan Charles LLOYD, *et al.*
Serial No. 10/705,242
December 15, 2008

188. (New) Apparatus as in claim 182, wherein said object attribute data includes data indicating whether each of said attributes is associated with one or more other attributes.

189. (New) Apparatus as in claim 182, wherein said attribute data includes data indicating whether each of said attributes is a sponsoring attribute for one or more other attributes.

190. (New) Apparatus as claimed in claim 182, wherein attributes having directory object naming characteristics in common are stored together.

191. (New) Apparatus as in claim 190, wherein the directory object naming characteristics correspond to one of: distinguished name attributes, aliased distinguished names, and non-naming attributes.

192. (New) Apparatus as in claim 190, wherein one of the intelligent directory services provides security services and uses its own security attribute data corresponding

Alan Charles LLOYD, *et al.*
Serial No. 10/705,242
December 15, 2008

to one of: collective attributes, compound attributes, attributes of compound attributes, X.500/LDAP operational attributes, user operational attributes, sponsoring attributes.

193. (New) Apparatus as in claim 182, wherein said segments include a first segment for storing distinct name binding rules, access control information, object schema and management data for said directory objects.

194. (New) Apparatus as in claim 193, wherein one of the intelligent directory services provides configuration services with said schema and management data to configure said object attribute data according to processing requirements of said intelligent directory services.

195. (New) Apparatus as in claim 186, wherein:
the directory system generates a directory operation access control identifier for use in determining whether a user is granted access to perform a selected directory operation on a selected attribute type in a selected portion of a DIT, said directory operation access control identifier identifying said directory operation, said portion of said DIT and said attribute type, and

the directory system determines whether said access is granted on the basis of a comparison of said directory operation access control identifier with one or more access control identifiers associated with one or more of said portion of said DIT, said attribute type, and an attribute type group including said attribute type.

196. (New) Apparatus as in claim 182, wherein

the directory system is adapted to generate one or more access control identifiers for a user on the basis of access configuration information for a user, and

a trusted operating system is used to determine said user's access to a directory object on the basis of access control identifiers associated with said object and said user.

197. (New) Apparatus as in claim 182, wherein said memory segments include transaction segments dedicated to storage of transaction data representing phases of a directory transaction to allow recovery of said directory transaction.

198. (New) Apparatus as in claim 182, including an adaptation component for automatically reconfiguring said memory segments on the basis of usage of said memory segments.

Alan Charles LLOYD, *et al.*
Serial No. 10/705,242
December 15, 2008

199. (New) Apparatus as in claim 182, wherein said memory segments include at least one adaptation segment dedicated to storage of adaptation data representing the usage of said memory segments.

200. (New) Apparatus as in claim 199, wherein said adaptation data represents the organization of directory data stored in said memory segments.

201. (New) Apparatus as in claim 198, wherein said reconfiguring includes segregating one or more portions of said directory data on the basis of access frequencies for said one or more portions of said directory data.

202. (New) Apparatus as in claim 198, wherein said reconfiguring includes segregating one or more portions of directory data based on the number of instances of an entity of said directory data in a region of memory.

203. (New) Apparatus as in claim 198, wherein said reconfiguring includes segregating instances of an attribute type from a name space into two or more regions of memory.

Alan Charles LLOYD, *et al.*
Serial No. 10/705,242
December 15, 2008

204. (New) Apparatus as in claim 182, including intelligent directory service modules for accessing and managing said plurality of memory segments.

205. (New) Apparatus as in claim 204, including a composite attribute module for managing composite attributes and extracting from said composite attributes particular attributes for storage in an associated object attribute data segment.

206. (New) Apparatus as in claim 204, including a statistical module for generating statistical data in relation to directory entries.

207. (New) Apparatus as in claim 204, including a monitoring module for monitoring one or more directory entries and for generating notification data in response to modification of a monitored directory entry.

208. (New) Apparatus as in claim 204, including a collective attributes module for segregating collective attributes of entries within a name space.

Alan Charles LLOYD, *et al.*
Serial No. 10/705,242
December 15, 2008

209. (New) Apparatus as in claim 204, including a X.509 certificate validation module for validating one or more certificate paths.

210. (New) Apparatus as in claim 204, including a multi-object management module for processing two or more objects as an entity.

211. (New) Apparatus as in claim 210, wherein said two or more objects include a sponsoring object and one or more sponsored objects.

212. (New) Apparatus as in claim 211, wherein said multi-object management module is adapted to automatically generate said one or more sponsored objects when a sponsoring object is generated.

213. (New) Apparatus as in claim 212, wherein said multi-object module is adapted to automatically generate one or more objects related to a user object when said user object is generated.

10/705,242

Alan Charles LLOYD, *et al.*
Serial No. 10/705,242
December 15, 2008

214. (New) Apparatus as in claim 213, wherein said user object represents a user, and said one or more objects represent one or more services for said user.

215. (New) Apparatus as in claim 182, including a service authorization module for determining whether a user is authorized to use one or more services.

216. (New) Apparatus as in claim 215, wherein said service authorization module is adapted to perform said determining in response to a directory search.

217. (New) Apparatus as in claim 216, wherein said directory search is based on an authorization matching rule, service and device properties, and an authorization token.

218. (New) Apparatus as in claim 182, including a relational search module for performing a distributed object relational search in response to a search query including relational operators.

219. (New) Apparatus as in claim 182, wherein the identity-based service components include a user presence management component that maintains presence

Alan Charles LLOYD, *et al.*
Serial No. 10/705,242
December 15, 2008

attributes of said users, said presence attributes including an attribute that indicates whether a user is using a directory.

220. (New) Apparatus as in claim 219, wherein said user presence management component generates one or more events in response to a change in said user presence attributes for each user.

221. (New) Apparatus as in claim 182, wherein the message-based service component includes a message transfer component that enables the message attributes of said directory objects to be transferred to other directory objects.

222. (New) Apparatus as in claim 182, including at least one attribute processor adapted to store and process attribute data of a directory.

223. (New) Apparatus as in claim 222, wherein said attribute processor includes an application-specific integrated circuit.